DAD SOCIAL MEDIA POLICY

भारत सरकार
रक्षा मंत्रालय
रक्षा लेखा विभाग

GOVERNMENT OF INDIA
MINISTRY OF DEFENCE
DEFENCE ACCOUNTS DEPARTMENT

सत्यमेव जयते

स्वच्छ भारत
एक कदम स्वच्छता की ओर

<u>FOREWORD</u>

Defence Accounts Deptt has been providing financial and audit services to the Armed forces of India for more than 250 years. The department has always worked to the satisfaction of its clients. However, in order to improve service delivery, use of social media is imperative. Social media will help DAD in connecting with the stakeholders in a much better, personalized and effective manner. Moreover, through social media, it will be possible to address the issues and concerns of our clients with an individual touch. Therefore, need for a policy was felt. DAD Social Media Policy has been framed in accordance with "Social Media Framework and Guidelines" issued by Ministry of Electronics and Information Technology. This policy document will help the department to use social media in an effective and secure way for leveraging its benefits.

(R P Singh)
Jt. CGDA (IT&S)

2

Contents

1. Objectives:

The objective for the use of social media is not just to disseminate information but also to undertake client engagement for a meaningful participation for effective formulation of policies and to improve our services.

Therefore, in DAD, Social Media may be used for:
- Generating awareness on various rules and regulations, Orders, OMs etc.
- Issue based as well as generic interaction
- Managing perceptions of our department (to avoid propagation of unverified facts, rumors with respect to government/department policies)

2. Platforms:

Various social media platforms are available on internet. Broadly, following platforms may be used by the department:

- Twitter
- Facebook
- YouTube
- Instagram

It is not necessary for the department to have accounts on all of the above mentioned platforms.

3. Governance Structure:

There will be only one social media account of the department on a particular platform. This will be maintained and operated from DAD HQrs. Approval of CGDA shall be taken for any matter related to social media account/handle of the department.

3.1 Account Governance:

Account Creation: A social media account establishes an organization's online identity.

Wherever possible, the same name for the different social networking accounts may be adopted to ensure ease of search on the internet. Another important facet of online identity is the need for it to be rendered effectively in either long form e.g. website address or in 15 characters or less (this is the Twitter maximum).

<u>Login and passwords</u>: A proper and secure record of login ids and password must be maintained. This is critical as multiple people may be authorized to post on behalf of the department/office.

<u>Account Status</u>: All the social media posts of Defence Accounts Department shall be posted only through official account(s) by officials who have been nominated by the competent authority.

<u>Responsiveness</u>: This indicates that how often would the pages/information be updated, in what manner would the responses be posted, what would be the turnaround time of responses etc. All of the social media accounts of the department shall be updated on weekly basis or as and when major events occur. This may include any important decision of MoD/CGDA or any new development.

<u>Response</u>:

- Not all posts/comments need to be responded to immediately and individually. Also, wherever a response is required all posts should be kept short and to the point.
- Responses shall only be made by the official account of that particular office. Employees should refrain themselves from responding through their personal accounts.
- Competent authority shall nominate the officials who will make the responses.
- For making a post or replying to a comment, approval of the competent authority shall invariably be taken by the social medial cell.
- In no circumstances, sensitive and confidential information shall be posted.

3.2 Content Governance:

<u>Accessibility</u>: In order to enable wider participation, content creation and availability should be in Indian languages and must not be limited to text alone. The content should follow the Government of India Guidelines for Website and adequately address challenges related to accessibility in Indian Languages as well as accessibility of content for differently abled.

<u>Records Management</u>: When any information is shared or guidance given online, it is necessary to ensure that all relevant records are captured, trail is generated and records are managed appropriately.

Following points may be kept in mind for Records management:

1. Records may be created on internal platform of the respective office and may be maintained with appropriate tags e.g. creator/sender, dates, posting site etc.
2. Screenshots may be captured and stored in soft or hard (copy) format and filed at appropriate place.
3. A summary may be created of the information/consultation and filed.

4. Institutionalisation of Social Media

A very important step is ensuring that the social media platform is integrated to the existing administrative and communication structure.
An indicative list includes:

- Achievements of the DAD.
- Any new initiatives of the DAD.
- Training related content of the department including DFMC activities.
- All important occasions as far as possible may be broadcasted using social media;
- All updates from the website would automatically be updated on social media sites;
- All traditional communications will publicise the social media presence.

5. What shall not be published/posted:

Personal information:

As per IT Act 2000, following types of personal information have been categorized as sensitive:

- password;
- financial information such as Bank account or credit card or debit card or   other payment instrument details;
- physical, physiological and mental health condition;
- sexual orientation;
- medical records and history;
- Biometric information;

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

- Sensitive information/data like budget, expenditure, details of procurement, movement details of defence personnel etc.
- Official noting, secret and confidential correspondences.
- Comments on any matter which is not yet finalized.
- Personal opinion.

6. Conclusion

The Framework and Guidelines in this document have been formulated with a view to make use of social media platforms to engage more meaningfully with its various stakeholders. Social media's characteristics of connectedness, collaboration and community have the potential of ensuring broad based consultation, and can help the department reduce the duration of consultation process and receive immediate feedback on services delivered. However, this is a dynamic and evolving area and continuous engagement and nimbleness of response to such an evolving scenario will determine the success of such efforts.